



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|----------------------|---------------------------|------------------------|
| 10/762,364 | 01/23/2004 | Roger Maitland | 50935-4/aba | 4471 |
| 7380 | 7590 | 07/11/2007 | | |
| SMART & BIGGAR P.O. BOX 2999, STATION D 900-55 METCALFE STREET OTTAWA, ON K1P5Y6 CANADA | | | EXAMINER TRAN, ELLEN C | |
| | | | ART UNIT 2134 | PAPER NUMBER |
| | | | MAIL DATE 07/11/2007 | DELIVERY MODE PAPER |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/762,364

Applicant(s)

MAITLAND ET AL.

Examiner

Ellen C. Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 January 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-76 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-76 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.



Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 8 Nov'04 & 18 Jun'04.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

Art Unit: 2134

DETAILED ACTION

1. This action is responsive to: an original application filed on 23 January 2004.
2. Claims 1-76 are pending; claims 1, 12, 21, 35, 49-51, 55, 64, and 73-76, are independent claims.
3. The IDS submitted 18 June 2004 and 8 November 2004 has been considered.

Claim Objections

4. Claims 1-50, are objected to because of the following informalities: the claims all indicate "for each of a plurality of look-up tables" this is confusing to the meaning of the claims because it is not clear what the phrase "for each of" is referring to. Appropriate correction is required. It is recommended the phrase "for each of" be deleted.
5. Claims 51-54, are objected to because independent claim 51 contains the phrase "permutation/reordering" this is indefinite because the slash ("/") typically indicates 'and or'. Appropriate correction is required.

Claim Objections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
7. Claims 15 and 18, are objected to under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Art Unit: 2134

8. Claims 15 and 18, contain the trademark/trade name Altivec. Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph. See *Ex parte Simpson*, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, the trademark/trade name is used to identify/describe a co-processor having a vperm instruction and, accordingly, the identification/description is indefinite.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. **Claims 1, 2, 5, 6, 11-13, 16, 21-28, 30, 31, 33-42, 44, 45, and 47-76,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al. World Intellectual Property Organization No. WO 03/050784 (hereinafter '784) International Filing Date 17 April 2002 in view of Luyster U.S. Patent No. 6,751,319 (hereinafter '319).

Art Unit: 2134

As to independent claim 1, "A method comprising: responsive to a plurality of inputs, each input being defined by a first set of bits and a second set of at least one bit, for each input of the plurality of inputs and in parallel with other inputs of the plurality of inputs:" is taught in '784 on page 9, lines 8-31, note simultaneously is interpreted to be equivalent to in parallel;

"and selecting a corresponding output from the set of corresponding outputs using the second set of a least one bit that defines the input" is shown on page 9, lines 13-31; the following is not explicitly taught in '784:

"for each of a plurality of look-up tables each having a plurality of elements, looking-up one of the plurality of elements of the look-up table using the first set of bits that define the input to obtain an output, the output from each of the plurality of look-up tables collectively comprising a set of corresponding outputs" however '319 teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51.

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm taught in '784 to include a means to utilize look-up tables. One of ordinary skill in the art would have been motivated to perform such a modification in order to save memory see '319 (col. 4, line 54 through col. 5, line 3) "A good example of perhaps the first historically significant symmetric cryptographic system (i.e., when the same key is used in the encipherment and decipherment transformations) is the Data Encryption Standard ("DES"), which is a U.S. Government standard.' DES uses small "s-boxes" to provide security. These so-called s-boxes are substitution boxes or, simply, look-up tables. S-boxes provide output which is a nonlinear function of the input, based on a lookup

table. Small s-boxes are lookup tables with a small number of possible inputs. Often, small s-boxes have a small number of output bits as well. For example, each s-box of DES has 6-bit inputs or 64 possible inputs and 4-bit outputs or 16 possible output values. They do not require much memory; nor does it take long to load them in microprocessor memory. S-boxes are generally stored in on-chip cache, generally the next quickest form of microprocessor memory after registers”.

As to dependent claim 2, “wherein the plurality of elements of each look-up table collectively comprise a combined table of elements each having a pre-determined value obtained using an S7 function” is taught in ‘784 page 11, lines 4-10.

As to dependent claim 5, “wherein for each of the plurality of inputs, the second set of at least one bit that defines the input comprises one bit and the set of corresponding outputs comprises two corresponding outputs, and wherein for each of the plurality of inputs the selecting comprises: selecting one of the two outputs using the one bit of the at least one bit that defines the input” is taught in ‘784 page 4, lines 30-35.

As to dependent claim 6, “wherein for each of the plurality of inputs, the second set of at least one bit that defines the input comprises at least two bits, and wherein for each of the plurality of inputs the selecting comprises: successively performing a selection on a remaining number of corresponding outputs of the set of corresponding outputs for each bit of the at least two bits, the number of corresponding outputs remaining being equal to all of the corresponding outputs of the set of corresponding outputs a first time the selection is performed, the selection being replacing the remaining number of corresponding outputs with a selection of half of the remaining number of outputs using a

Art Unit: 2134

respective bit of the at least two bits, the selection of half of the remaining number of outputs being the number of remaining outputs for the next time the selection is performed” is shown in ‘784 page 6, lines 8-29.

As to dependent claim 11, “applied in ciphering data in a Kasumi implementation” is taught in ‘784 page 2, lines 25-33.

As to independent claim 12, this claim is directed to the apparatus executing the method of claim 1; therefore it is rejected along similar rationale.

As to dependent claims 13 and 16, these claim contain substantially similar subject matter as claims 2, 5, and 6; therefore they are rejected along similar rationale.

As to independent claim 21, “A method comprising: responsive to a plurality of inputs, each input being defined by a first plurality of bits, for each input of the plurality of inputs and in parallel with other inputs of the plurality of inputs:” is taught on page 9, lines 8-31, note simultaneously is interpreted to be equivalent to in parallel;

“selecting a respective subset of bits of the first plurality of bits that define the input, the bits of the respective subset of bits comprising fewer bits than the first plurality of bits of the input” is shown on page 9, lines 13-31;
the following is not explicitly taught in ‘784:

“for each of a plurality of look-up tables each having a plurality of elements” and “and looking-up an element of the plurality of elements of the look-up table using the subset of bits to obtain an output; and combining the outputs obtained from the plurality of look-up tables to obtain at least one bit” however ‘319 teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51.

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm taught in '784 to include a means to utilize look-up tables. One of ordinary skill in the art would have been motivated to perform such a modification in order to save memory see '319 (col. 4, line 54 through col. 5, line 3) "A good example of perhaps the first historically significant symmetric cryptographic system (i.e., when the same key is used in the encipherment and decipherment transformations) is the Data Encryption Standard ("DES"), which is a U.S. Government standard. DES uses small "s-boxes" to provide security. These so-called s-boxes are substitution boxes or, simply, look-up tables. S-boxes provide output which is a nonlinear function of the input, based on a lookup table. Small s-boxes are lookup tables with a small number of possible inputs. Often, small s-boxes have a small number of output bits as well. For example, each s-box of DES has 6-bit inputs or 64 possible inputs and 4-bit outputs or 16 possible output values. They do not require much memory; nor does it take long to load them in microprocessor memory. S-boxes are generally stored in on-chip cache, generally the next quickest form of microprocessor memory after registers".

As to dependent claim 22, "wherein for each input of the plurality of inputs, the outputs obtained from the plurality of look-up tables each comprise a second plurality of bits, the second plurality of bits comprising fewer bits than the first plurality of bits of the input" is shown in '784 page 10, lines 9-15.

As to dependent claim 23, "wherein for each input of the plurality of inputs, the at least one bit comprises a third plurality of bits, the third plurality of bits comprising the

same number of bits as the first plurality of bits of the input” is shown in ‘784 page 10, lines 9-15.

As to dependent claim 24, “wherein for at least one look-up table of the plurality of look-up tables, for each input the selecting comprises manipulating at least one of the plurality of bits that define the input using at least one of a bit rotation instruction and a bit shifting instruction” is disclosed in ‘784 page 6, lines 1-29.

As to dependent claim 25, “wherein for each of the at least one look-up table, for each input the manipulating at least one of the first plurality of bits comprises ordering the respective subset of bits of the input as least significant bits” is taught in ‘784 page 9, lines 7-31.

As to dependent claim 26, “wherein each element of the plurality of elements of each look-up table has a pre-determined value” however ‘319 teaches loading predetermined values into tables in col. 38, lines 24-36.

As to dependent claim 27, “wherein for each input of the plurality of inputs the first plurality of bits and the third plurality of bits each comprise 9 bits, the pre-determined value of each of the plurality of elements of each of the plurality of look-up tables is obtained from a partial evaluation of an S9 function” is shown in ‘784 page 9, line 32 through page 10, line 8.

As to dependent claim 28, “wherein for each look-up table of the plurality of look-up tables, the pre-determined value of each of the plurality of elements of the look-up table is a function of a number being definable by a bit sequence of one of 4 and 5 bits” is disclosed in ‘784 page 13, lines 9-16.

As to dependent claim 30, “wherein for each input of the plurality of inputs, the combining comprises performing a plurality of exclusive-OR operations on the outputs obtained from the plurality of look-up tables for the input” is taught in ‘784 page 9, lines 9-31.

As to dependent claim 31, “wherein for each input of the plurality of inputs, the combining comprises manipulating the second plurality of bits of at least one output of the outputs obtained from the plurality of look-up tables for the input using one of a bit shifting instruction and a bit rotation instruction” is shown in ‘784 page 9, lines 9-31.

As to dependent claim 33, “wherein for each input of the plurality of inputs, the combining comprises: for a first output of the outputs obtained from the plurality of look-up tables for the input, manipulating the second plurality of bits of the first output using one of a bit rotation instruction and a bit shifting instruction; and for a second output of the outputs obtained from the plurality of look-up tables for the input, performing one of the plurality of exclusive-OR operations on the second output and the first output to obtain a third output having a fourth plurality of bits” is disclosed in ‘784 page 9, lines 9-31.

As to dependent claim 34, “wherein for each input, the bits of the second plurality of bits of each respective subset of bits of the first plurality of bits of the input have a pre-determined order and are each used for obtaining a respective one of the third plurality of bits, the outputs obtained from the look-up tables collectively comprising at least one group of outputs each having at least two outputs of the outputs obtained from the look-up tables” however ‘319 teaches lookup tables in col. 15, lines 48-55;

“for each group of outputs of the at least one group of outputs the at least two outputs in the group of outputs having bits used for determining a common subset of bits of the third plurality of bits, the combining comprising: for each group of outputs of the at least of group of outputs, combining the at least two outputs of the group of outputs using at least one of the plurality of exclusive-OR operations” is shown in ‘784 page 5, lines 10-36.

As to independent claim 35, this claim is directed to the apparatus executing the method of claim 21; therefore it is rejected along similar rationale.

As to dependent claims 36-42, 44, 45, 47, and 48, these claim contain substantially similar subject matter as claims 22-28, 30, 31, 33, and 34; therefore they are rejected along similar rationale.

As to independent claim 49, this claim is directed to an article of manufacture of the method of claim 1; therefore it is rejected along similar rationale.

As to independent claim 50, this claim is directed to an article of manufacture of the method of claim 21; therefore it is rejected along similar rationale.

As to independent claim 51, **“A method comprising: responsive to N K_{in} -bit inputs: performing bit permutation/reordering on the N K_{in} -bit inputs to produce M parallel sets of outputs wherein N and K_{in} are integers satisfying $N, K_{in} \geq 2$, an i th set of outputs of the M parallel sets of outputs containing N sets of bits $L_{i,in}$ bits in length with i and $L_{i,in}$ being integers satisfying $i=1$ to M and $1 \leq L_{i,in} < K_{in}$, the i th set of outputs defining a respective subset of the K_{in} bits of the inputs”** is taught on page 9, lines 8-31, note simultaneously is interpreted to be equivalent to in parallel;

Art Unit: 2134

“ $L_{i,out}$ being an integer satisfying $L_{i,out} \geq 1$; and for each of the N K_{in} -bit inputs, generating a respective output by performing a bit combining operation on the outputs from the parallel look-up table operations associated with the input” is shown on page 9, lines 13-31;

the following is not explicitly taught in ‘784:

“for each parallel set of outputs, performing a parallel lookup table operation to generate a corresponding parallel set of outputs containing N outputs, each being associated with a respective one of the N K_{in} -bit inputs and each being $L_{i,out}$ bits in length” however ‘319 teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51.

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm taught in ‘784 to include a means to utilize look-up tables. One of ordinary skill in the art would have been motivated to perform such a modification in order to save memory see ‘319 (col. 4, line 54 through col. 5, line 3) “ A good example of perhaps the first historically significant symmetric cryptographic system (i.e., when the same key is used in the encipherment and decipherment transformations) is the Data Encryption Standard ("DES"), which is a U.S. Government standard. DES uses small "s-boxes" to provide security. These so-called s-boxes are substitution boxes or, simply, look-up tables. S-boxes provide output which is a nonlinear function of the input, based on a lookup table. Small s-boxes are lookup tables with a small number of possible inputs. Often, small s-boxes have a small number of output bits as well. For example, each s-box of DES has 6-bit inputs or 64 possible inputs and 4-bit outputs or 16 possible output values. They do not require

Art Unit: 2134

much memory; nor does it take long to load them in microprocessor memory. S-boxes are generally stored in on-chip cache, generally the next quickest form of microprocessor memory after registers”.

As to dependent 52, “wherein for each of the N K_{in} -bit inputs, the generating comprises performing a bit manipulation on the outputs of the parallel look-up table operations associated with the input” is disclosed in ‘784 page 6, lines 1-29.

As to dependent 53, “wherein the bit combining operations are implemented in parallel” is taught in ‘784 on page 9, lines 8-31, note simultaneously is interpreted to be equivalent to in parallel.

As to dependent claim 54, “wherein for each of the N K_{in} -bit inputs the respective output generated K_{out} bits, K_{out} being an integer satisfying $K_{out} \geq 1$, and wherein in performing the bit permutation/reordering on the N K_{in} -bit inputs, the i th set of outputs defining the respective subset of the K_{in} bits of the inputs is selected such that the respective subset of the K_{in} bits effects only a defined maximum number $P_i < K_{out}$ bits of the respective outputs wherein P_i is an integer” is disclosed in ‘784 page 6, lines 1-29.

As to independent claim 55, “A method of generating a plurality of outputs according to a ciphering algorithm which for each of the plurality of outputs operates on a respective input using a respective key, the ciphering algorithm comprising a plurality of rounds in which functions are evaluated, the method comprising, for at least one function of the functions of at least one of the plurality of rounds: responsive to a plurality of first inputs each being associated with one of the respective inputs, for each first input and in

Art Unit: 2134

parallel with other first inputs of the plurality of first inputs:" is taught on page 9, lines 8-31, note simultaneously is interpreted to be equivalent to in parallel; the following is not explicitly taught in '784:

"generating an output by looking up at least one look-up table using the input, each look-up table having a plurality of elements" however '319 teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51.

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm taught in '784 to include a means to utilize look-up tables. One of ordinary skill in the art would have been motivated to perform such a modification in order to save memory see '319 (col. 4, line 54 through col. 5, line 3) " A good example of perhaps the first historically significant symmetric cryptographic system (i.e., when the same key is used in the encipherment and decipherment transformations) is the Data Encryption Standard ("DES"), which is a U.S. Government standard. DES uses small "s-boxes" to provide security. These so-called s-boxes are substitution boxes or, simply, look-up tables. S-boxes provide output which is a nonlinear function of the input, based on a lookup table. Small s-boxes are lookup tables with a small number of possible inputs. Often, small s-boxes have a small number of output bits as well. For example, each s-box of DES has 6-bit inputs or 64 possible inputs and 4-bit outputs or 16 possible output values. They do not require much memory; nor does it take long to load them in microprocessor memory. S-boxes are generally stored in on-chip cache, generally the next quickest form of microprocessor memory after registers".

As to dependent claim 56, “wherein the ciphering algorithm is a Kasumi algorithm” is taught in ‘784 page 2, lines 25-33.

As to dependent claim 57, “wherein for a function of a certain type of the at least one function the at least one look-up table comprising a plurality of look-up tables and the output from each of the plurality of look-up tables collectively comprising a set of corresponding outputs” however ‘319 teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51;

“each first input of the plurality of first inputs being defined by a first set of bits and a second set of at least one bit, the method comprising for each first input of the plurality of first inputs and in parallel with the other first inputs of the plurality of first inputs:” is taught in ‘784 on page 9, lines 8-31;

“selecting a corresponding output from the set of corresponding outputs using the second set of at least one bit that defines the input” is shown in ‘784 page 6, lines 8-29.

As to dependent claim 58, “wherein the ciphering algorithm is a Kasumi algorithm and the function of a certain type is an S7 function” is taught in ‘784 page 11, lines 4-10.

As to dependent claim 59, “wherein for a function of a certain type of the at least one function the at least one look-up table comprises a plurality of look-up tables and each first input of the plurality of first inputs is defined by a first plurality of bits, the method comprising:” however ‘319 teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51;

“for each first input of the plurality of first inputs and in parallel with the other first inputs of the plurality of first inputs: for each of the plurality of look-up tables: selecting a respective subset of bits of the first plurality of bits that define the first input, the bits of the respective subset of bits comprising fewer bits than the first plurality of bits of the first input, the look-up table being looked up using the subset of bits to obtain the output” is shown in ‘784 page 6, lines 8-29;

“and combining the outputs obtained from the plurality of look-up tables to obtain at least one bit” is taught in ‘784 page 2, lines 25-33.

As to dependent claim 60, **“wherein the ciphering algorithm is a Kasumi algorithm and the function of a certain type is an S9 function”** is taught in ‘784 page 11, lines 4-10.

As to dependent claim 61, **“wherein the at least one round comprises the plurality of rounds and wherein for each round the at least one function comprises six S7 functions and six S9 functions, the method further comprising for each function of the plurality of functions other than the at least one function: responsive to a plurality of second inputs each being associated with one of the respective inputs, and in parallel with other second inputs of the plurality of second inputs: generating an output according to the function using the input”** is shown in ‘784 page 11, lines 4-36.

As to dependent claim 62, **“further comprising, for each output of the plurality of outputs and in parallel with other outputs of the plurality of outputs: combining the output with input data to generate ciphered data”** is taught in ‘784 on page 9, lines 8-31.

As to dependent claim 63, “wherein the combining comprises performing an exclusive-OR operation” is taught in ‘784 page 9, lines 9-31.

As to independent claim 64, this claim is directed to the apparatus executing the method of claim 55; therefore it is rejected along similar rationale.

As to dependent claims 65-72, these claims contain substantially similar subject matter as claims 56-63; therefore they are rejected along similar rationale.

As to independent claim 73, this claim is directed to an article of manufacture of the method of claim 55; therefore it is rejected along similar rationale.

As to independent claim 74, A method comprising: responsive to a plurality of inputs, each input being defined by at least one bit, for each input of the plurality of inputs and in parallel with other inputs of the plurality of inputs:” is taught on page 9, lines 8-31, note simultaneously is interpreted to be equivalent to in parallel; the following is not explicitly taught in ‘784:

“looking-up a look-up table having a plurality of elements using the at least one bit that define the input to obtain an output” however ‘319 teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51.

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm taught in ‘784 to include a means to utilize look-up tables. One of ordinary skill in the art would have been motivated to perform such a modification in order to save memory see ‘319 (col. 4, line 54 through col. 5, line 3) “ A good example of perhaps the first historically significant symmetric cryptographic

Art Unit: 2134

system (i.e., when the same key is used in the encipherment and decipherment transformations) is the Data Encryption Standard ("DES"), which is a U.S. Government standard. DES uses small "s-boxes" to provide security. These so-called s-boxes are substitution boxes or, simply, look-up tables. S-boxes provide output which is a nonlinear function of the input, based on a lookup table. Small s-boxes are lookup tables with a small number of possible inputs. Often, small s-boxes have a small number of output bits as well. For example, each s-box of DES has 6-bit inputs or 64 possible inputs and 4-bit outputs or 16 possible output values. They do not require much memory; nor does it take long to load them in microprocessor memory. S-boxes are generally stored in on-chip cache, generally the next quickest form of microprocessor memory after registers".

As to independent claim 75, this claim is directed to the apparatus executing the method of claim 74; therefore it is rejected along similar rationale.

As to independent claim 76, this claim is directed to an article of manufacture executing the method of claim 74; therefore it is rejected along similar rationale.

11. **Claims 3, 4, 7-10, 14,15, 17-20, 29, 32, 34, 43, and 46**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al. World Intellectual Property Organization No. WO 03/050784 (hereinafter '784) International Filing Date 17 April 2002 in view of Luyster U.S. Patent No. 6,751,319 (hereinafter '319) in further view of Weybrew et al. U.S. Patent No. 6,931,511 (hereinafter '511).

As to dependent claim 3, the following is not explicitly taught in '784 and '319:
"wherein for each look-up table, the plurality of elements of the look-up table and the plurality of inputs are loaded as vectors and the looking-up comprises for each of the

Art Unit: 2134

inputs selecting one of the plurality of elements of the look-up table using the first set of bits that define the input” however ‘511 teaches a plurality of look-up tables being loaded as vectors in col. 8, lines 37-56.

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm that utilizes look-up tables taught in the combination of ‘784 and ‘319 to include a means to utilize vectors as inputs. One of ordinary skill in the art would have been motivated to perform such a modification in because vector processing allows simultaneous processing of vector data see ‘511 (col. 4, line 5 et seq.) “Vector processors allow simultaneous processing of a vector of data elements using a single instruction. Table look-up for a vector of data elements maps the data elements of the vector into another vector of data elements using one or an array of tables. In one scenario, each data elements of a vector is looked up from a look-up table, and looking up the data element from the look-up table is independent of looking up other elements from other look-up tables and thus multiple look-ups are preformed sequentially over time”.

As to dependent claim 4, “comprising using a vperm (vector permutation) instruction for the selecting one of the plurality of elements of the look-up table using the first set of bits that define the input” however ‘511 teaches a vperm instruction in col. 29, lines 44-67.

As to dependent claim 7, “wherein for each time the selection on a remaining number of corresponding outputs is performed, the remaining number of corresponding outputs comprises at least one set of two remaining corresponding outputs and the selection of half of the remaining number of outputs comprises, for each set of two corresponding

outputs of the at least one set of two remaining corresponding outputs:” is shown in ‘784 page 2, lines 25-36;

“replicating the respective bit into a plurality of replicated bits; and using a vector instruction, selecting one of the two remaining corresponding outputs depending on the plurality of replicated bits” however ‘511 teaches utilizing vectors to select outputs in col. 8, lines 56-65.

As to dependent claim 8, “wherein the vector instruction is a vsel (vector select instruction)” however ‘511 shows a method to lookup data items indexed by a plurality of vectors in col. 8, lines 56-65.

As to dependent claim 9, “wherein for each input, the first set of bits that define the input comprises five bits, the second set of bits that define the input comprises two bits and the look-up tables comprise four look-up tables, wherein for each of the four look-up tables the plurality of inputs and the plurality of elements of the look-up table are loaded as vectors and the looking-up comprises for each of the inputs selecting one of the plurality of elements of the look-up table using the first set of bits that define the input” however ‘511 teaches vectors are loaded in a plurality of lookup tables in col 8, lines 37-67.

As to dependent claim 10, “wherein for each input, the first set of bits that define the input comprises four bits, the second set of bits that define the input comprises three bits and the look-up tables comprise eight look-up tables, and wherein for each of the eight look-up tables the plurality of inputs and the plurality of elements of the look-up table are loaded as vectors and for each of the inputs the looking-up comprises selecting one of the

plurality of elements of the look-up table using the first set of bits that define the input”

however ‘511 teaches that the vector are indices in col. 8, lines 37-56.

As to dependent claims 14, 15, 17-20, these claim contain substantially similar subject matter as claims 3, 4, 7-10; therefore they are rejected along similar rationale. Note an Altivec processor is shown in ‘511 col. 5, lines 36-46.

As to dependent claim 29, “wherein for each input of the plurality of inputs, for each look-up table the respective subset of bits of the first plurality of bits that define the input comprises one of 4 and 5 bits and the look-up table is looked-up using a vperm (vector permutation) instruction” however ‘511 teaches a vperm instruction in col. 29, lines 44-67.

As to dependent claim 32, “wherein the bit shifting instruction comprises one of a vector shift right byte instruction and a vector shift left byte instruction and the bit rotation instruction comprises one of a vector rotate left byte instruction and a vector rotate right byte instruction” however ‘511 teaches in col. 80, lines 17-41 a macro to rotate vector.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant’s disclosure.

Averbuj et al.

U.S. Patent No. 7,212,631

issued dated: May 01, 2007

Art Unit: 2134

13. inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Ellen Tran
Patent Examiner
Technology Center 2134
23 June 2007